



UNITED STATES DEPARTMENT OF STATE
AND THE BROADCASTING BOARD OF GOVERNORS
OFFICE OF INSPECTOR GENERAL

AUD-IT-IB-15-13

Office of Audits

October 2014

Audit of the Broadcasting Board of Governors Information Security Program

~~**IMPORTANT NOTICE:** This report is intended solely for the official use of the Department of State or the Broadcasting Board of Governors, or any agency or organization receiving a copy directly from the Office of Inspector General. No secondary distribution may be made, in whole or in part, outside the Department of State or the Broadcasting Board of Governors, by them or by other agencies or organizations, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code, 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~



OIG Office of Inspector General
U.S. Department of State • Broadcasting Board of Governors

(U) PREFACE

(U) This report is being transmitted pursuant to the Inspector General Act of 1978, as amended, and Section 209 of the Foreign Service Act of 1980, as amended. It is one of a series of audit, inspection, investigative, and special reports prepared as part of the Office of Inspector General's (OIG) responsibility to promote effective management, accountability, and positive change in the Department of State and the Broadcasting Board of Governors.

(U) In accordance with the Federal Information Security Management Act of 2002 (FISMA), OIG performed an audit of the Broadcasting Board of Governors Information Security Program for FY 2014. To perform this audit, OIG contracted with the independent public accountant Williams, Adley & Company, LLP. The audit report is based on interviews with employees and officials of the Broadcasting Board of Governors, direct observation, and a review of applicable documents.

(U) The independent public accountant identified areas in which improvements could be made, including the risk management program, continuous monitoring, contingency planning, incident response and reporting, plans of actions and milestones, remote access management, configuration management, identity and access management, and security training and awareness.

(U) OIG evaluated the nature, extent, and timing of the independent public accountant's work; monitored progress throughout the audit; reviewed supporting documentation; evaluated key judgments; and performed other procedures as appropriate. OIG concurs with the findings, and the recommendations contained in the audit report were developed based on the best knowledge available and discussed in draft form with those individuals responsible for implementation. OIG's analysis of management's response to the recommendations has been incorporated into the report. OIG trusts that this report will result in more effective, efficient, and/or economical operations.

(U) I express my appreciation to all of the individuals who contributed to the preparation of this report.

A handwritten signature in blue ink, appearing to read "N. P. Brown".

(U) Norman P. Brown
(U) Assistant Inspector General
for Audits



Audit of the Broadcasting Board of Governors Information Security Program

October 22, 2014

Office of Inspector General
U.S. Department of State and the Broadcasting Board of Governors
Washington, DC

Williams, Adley & Company-DC, LLP has performed an audit of the Broadcasting Board of Governors' (BBG) Information Security Program. We audited the Department's compliance with the Federal Information Security Management Act, Office of Management and Budget requirements, and National Institute of Standards and Technology standards. We performed this audit under Contract No. SAQMMA10F2159. The audit was designed to meet the objectives described in the report.

We conducted this performance audit in accordance with *Government Auditing Standards*, issued by the Comptroller General of the United States. We communicated the results of our audit and the related findings and recommendations to the U.S. Department of State and the Broadcasting Board of Governors Office of Inspector General.

We appreciate the cooperation provided by BBG personnel during the audit.

Williams, Adley & Company-DC, LLP

WILLIAMS, ADLEY & COMPANY-DC, LLP
Certified Public Accountants / Management Consultants
1030 15th Street, NW, Suite 300W • Washington, DC 20005 • (202) 371-1397 • Fax: (202) 371-9161
www.williamsadley.com

(U) Acronyms

(U) AD	Active Directory
(U) BBG	Broadcasting Board of Governors
(U) DHS	Department of Homeland Security
(U) FISMA	Federal Information Security Management Act
(U) IT	Information Technology
(U) NIST	National Institute of Standards and Technology
(U) OIG	Office of Inspector General
(U) OMB	Office of Management and Budget
(U) PIV	Personal Identity Verification
(U) POA&M	Plans of Action and Milestones
(U) SP	Special Publication
(U) VPN	Virtual Private Network

(U) TABLE OF CONTENTS

(U) Executive Summary 1

(U) Background 2

(U) Objective 3

(U) Results of Audit..... 3

 (U) Finding A. BBG Has Not Enforced Its Risk Management Framework..... 3

 (U) Finding B. BBG Has Not Finalized a Continuous Monitoring Policy..... 5

~~(SBU)~~ Finding C. BBG Has Not Finalized and Implemented Contingency Plans..... 6

 (U) Finding D. BBG Has Not Implemented Effective Configuration Management Policies .. 7

 (U) Finding E. BBG Has Not Implemented an Effective Incident Response and Reporting Program..... 10

 (U) Finding F. BBG Has Not Fully Followed Its Plans of Action and Milestones Policy..... 12

 (U) Finding G. BBG’s Remote Access Controls Can Be Improved..... 13

 (U) Finding H. BBG Has Not Implemented Effective Identity and Access Management Practices 14

 (U) Finding I. BBG’s Security Training Policy Did Not Contain Role-Based Training..... 16

 (U) Finding J. BBG Has Complied with Contractor Oversight and Security Capital Planning Requirements 17

(U) List of Recommendations..... 18

(U) Appendices

 (U) A. Scope and Methodology 20

 (U) B. Followup of Recommendations from the FY 2013 Audit of the Broadcasting Board of Governors Information Security Program 25

 (U) C. Broadcasting Board of Governors Response..... 28

(U) Executive Summary

(U) In accordance with the Federal Information Security Management Act of 2002 (FISMA),¹ the Office of Inspector General (OIG) contracted with Williams, Adley & Company-DC, LLP (referred to as “we” in this report), to perform an independent audit of the Broadcasting Board of Governors (BBG) information security program’s compliance with Federal laws, regulations, and standards established by FISMA, the Office of Management and Budget (OMB), and the National Institute of Standards and Technology (NIST). See Appendix A for more information on our audit scope and methodology. We found that BBG was substantially not in compliance with FISMA, OMB, and NIST requirements.

(U) Collectively, the information security control weaknesses we identified in this audit represent a significant deficiency² to enterprise-wide security, as defined by OMB Memorandum M-14-04.³ We identified control weaknesses in 9 of the 11 information security program areas that considerably impacted BBG’s information security program. The most significant information security deficiencies are related to the risk management framework, continuous monitoring program, [REDACTED] contingency plans, configuration management, and the incident response and reporting program. In addition, information security program areas that need improvement include Plans of Action and Milestones (POA&M), remote access, identity and access management, and security training. Since FY 2010, the weak (and in some cases lack of) security controls adversely affected the confidentiality, integrity, and availability of information and information systems. As an example, according to a BBG official, the weak security controls resulted in the hacking of BBG Web sites in 2011.

(U) In FY 2014, BBG continued to implement some controls to improve its information security program. For example, BBG categorized system information types and included applicable NIST Special Publication (SP) 800-53 controls in the security plans to improve the risk management process. BBG also added additional data fields in the POA&M database to track and remediate corrective actions. In addition, BBG has continued to be in compliance with contractor oversight requirements and has established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to BBG. For security capital planning, there have been no major Information Technology (IT) investments or capital investments funding in FY 2014.

(U) The FY 2013 FISMA report⁴ contained 13 recommendations intended to address security deficiencies. We reviewed BBG’s corrective actions to address the weaknesses identified in the FY 2013 FISMA report and recognize that BBG has taken steps to improve its

¹ (U) Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (2002).

² (U) According to OMB Memorandum M-14-04, a significant deficiency is defined as a weakness in an agency’s overall information systems security program or management control structure, or within one or more information systems that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets.

³ (U) OMB Memorandum M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013.

⁴ (U) OIG, AUD-IT-IB-14-02, *Audit of the Broadcasting Board of Governors Information Security Program*, October 2013.

information security program. Based on actions identified during the audit, OIG closed 2 of 13 recommendations contained in the FY 2013 report (see Appendix B, “Followup of Recommendations from the FY 2013 Audit of the Broadcasting Board of Governors Information Security Program”). To further improve its information security program, we are making 18 recommendations to BBG in 9 of 11 reportable FISMA areas.

(U) In its October 17, 2014, response to the draft report (see Appendix C), BBG concurred with 17 of the 18 recommendations. Based on BBG’s response to the recommendations, OIG considers 17 recommendations resolved, pending further action, and 1 recommendation unresolved. BBG’s response and OIG’s reply are presented after each recommendation.

(U) Background

(U) BBG is an independent Federal agency supervising all U.S. Government-supported civilian international media whose mission is to inform, engage, and connect people around the world in support of freedom and democracy. Broadcasters within the BBG network include the Voice of America, Radio Free Europe/Radio Liberty, the Middle East Broadcasting Networks, Radio Free Asia, and the Office of Cuba Broadcasting. Voice of America and Office of Cuba Broadcasting are part of the Federal government. Radio Free Europe/Radio Liberty, Radio Free Asia, and Middle East Broadcasting Networks are surrogate broadcasters that receive grants but are organized and managed as private non-profit corporations. The Federal Acquisition Regulation, Part 7, *Acquisition Planning*,⁵ requires that agencies ensure information technology acquisitions comply with FISMA security requirements and, when applicable, agencies must also include FISMA’s security requirements in the terms and conditions of grants.

(U) With the passage of FISMA, Congress recognized the importance of information security to the economic and national security interests of the United States and required each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or source. FISMA provides a comprehensive framework for establishing and ensuring the effectiveness of management, operational, and technical controls over IT that supports Federal operations and assets, and it provides a mechanism for improved oversight of Federal agency information security programs.

(U) To strengthen information systems security, FISMA assigns specific responsibilities to the Department of Homeland Security (DHS), NIST, OMB, and other Federal agencies. In particular, FISMA requires the head of each agency to implement policies and procedures to cost-effectively reduce IT security risks to an acceptable level. To ensure the adequacy and effectiveness of information system controls, FISMA requires agency program officials, chief information officers, senior agency officials for privacy, and inspectors general to conduct annual reviews of the agency’s information security program and report the results to DHS.

⁵ (U) OMB Memorandum M-14-04, *FY 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 2013.

(U) On an annual basis, OMB provides guidance with reporting categories and questions to meet the current year's reporting requirements.⁶ OMB uses responses to its questions to assist in its oversight responsibilities and to prepare its annual report to Congress on agency compliance with FISMA.

(U) Objective

(U) The objective of this audit was to perform an independent evaluation of BBG's information security program and practices for FY 2014, which included testing the effectiveness of security controls for a subset of systems, as required.

(U) Results of Audit

(U) Overall, we identified control weaknesses in 9 of the 11 information security program areas that significantly impacted BBG's information security program. We recognize that BBG made progress in the risk management and POA&M areas since FY 2013, but even with the progress made, we found that BBG was still not in compliance with FISMA, OMB, and NIST requirements. Although BBG continued to be in compliance in two information security program areas, capital planning and contractor oversight, BBG's overall information security program has not been in compliance with FISMA, OMB, and NIST requirements since FY 2010.

(U) Finding A. BBG Has Not Enforced Its Risk Management Framework

(U) We have found deficiencies with BBG's risk management framework since FY 2010. According to NIST SP 800-37, Revision 1,⁷ BBG should conduct a privacy impact assessment on information systems in accordance with OMB policy. In addition, according to NIST SP 800-53, Revision 4,⁸ BBG should assess the security controls in an information system annually. However, in FY 2014, we identified the following weaknesses within the risk management framework that the Information Security Division should enforce:

- (U) Privacy impact assessments⁹ were not completed for the Office of Cuba Broadcasting Headquarters Network and Privacy Information Enclave systems.
- (U) An annual security control assessment was not conducted on the Identity Management System.

(U) According to a BBG official, system owners have not completed privacy impact assessments because BBG chose to prioritize resources to update and complete System Security

⁶ (U) DHS, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, December 2013.

⁷ (U) NIST SP 800-37, rev. 1, *Guide for Applying the Risk Management Framework to Federal Information Systems*, "Appendix F," February 2010.

⁸ (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, "CA-2 Security Assessments," April 2013 (last updated January 2014).

⁹ (U) The privacy impact assessment can be an appendix to the security plan submitted as part of the security authorization package.

Plans to comply with the most recent NIST guidance and obtain memorandums for Authority to Operate for the systems set to expire at the end of FY 2014. In addition, BBG's policy and procedures for certification and accreditation did not identify the organization responsible for assessing security controls on an annual basis.

(U) Without the Information Security Management Division enforcing a risk management framework, BBG cannot prioritize, assess, respond to, and monitor information security risk, which leaves BBG vulnerable to outside attacks and insider threats.

(U) Recommendation 1. OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Office of Cuba Broadcasting Headquarters Network system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) Management Response: BBG concurred with this recommendation and stated the Agency will perform a privacy impact assessment for the Office of Cuba Broadcasting system during FY 2015.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has performed a privacy impact assessment for the Office of Cuba Broadcasting system.

(U) Recommendation 2. OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Privacy Information Enclave system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) Management Response: BBG concurred with this recommendation and stated the Agency will perform a privacy impact assessment for the Privacy Information Enclave system during FY 2015.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has performed a privacy impact assessment for the Privacy Information Enclave system.

(U) Recommendation 3. OIG recommends that the Broadcasting Board of Governors update the Certification and Accreditation Policy and Procedures to identify the responsible organizations for conducting annual security control assessments.

(U) Management Response: BBG concurred with this recommendation and stated the Chief Information Officer will prioritize resources to ensure the Certification and Accreditation Policy and Procedures with the associated tracking sheets appropriately identify all responsible parties.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has

updated the Certification and Accreditation Policy and Procedures to identify the responsible organizations for conducting annual security control assessments.

(U) Recommendation 4. OIG recommends that the Broadcasting Board of Governors perform annual security control assessments on its Identity Management System.

(U) Management Response: BBG concurred with this recommendation and stated the Agency will work to complete all the required annual security assessments during FY 2015, as the Agency adopts the Risk Management Framework in the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has performed annual security control assessments on its Identity Management System.

(U) Finding B. BBG Has Not Finalized a Continuous Monitoring Policy

(U) Although BBG established a continuous monitoring strategy, the Office of the Director of Global Operations has not approved an overall continuous monitoring policy. According to NIST SP 800-53, Revision 4,¹⁰ organizations should establish a continuous monitoring strategy and implement a continuous monitoring policy. OMB¹¹ guidance states, “A well designed and well managed continuous monitoring program can effectively transform an otherwise static and occasional security control assessment and risk determination process into a dynamic process that provides essential, near real time security status related information” to senior leaders. Senior leaders can use this information to take “appropriate risk mitigation actions and make cost effective, risk based decisions regarding the operation of their information systems.”

(U) According to BBG’s Director of Global Operations,¹² the policy has not been approved because the Agency is still maturing its continuous monitoring program by participating in the DHS Continuous Diagnostics and Mitigation Program, which provides guidance to detect compliance and risk issues associated with BBG’s financial and operational environment. However, we determined that BBG was not scheduled for integration with the DHS Continuous Diagnostics and Mitigation Program until 2016. As a result, BBG currently has a continuous monitoring strategy that is deferring to the 2016 implementation of the DHS Continuous Diagnostics and Mitigation Program, but there is no continuous monitoring policy in place until the program is implemented. Not having an overall continuous monitoring policy hinders BBG’s ability to monitor the network environment and identify threats and vulnerabilities.

¹⁰ (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “CA-7 Continuous Monitoring,” April 2013 (last updated January 2014).

¹¹ (U) OMB, *Fiscal Year 2010 Report to Congress on the Implementation of The Federal Information Security Management Act of 2002*, “Continuous Monitoring and Remediation,” March 2010.

¹² (U) The Director of Global Operations also serves the function of BBG’s Chief Information Officer and acting Chief Financial Officer.

(U) **Recommendation 5.** OIG recommends that the Director of Global Operations approve and implement a continuous monitoring policy that assesses the security state of information systems and is consistent with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) **Management Response:** BBG concurred with this recommendation and stated the Chief Information Officer will continue to ensure that the continuous monitoring policy and the associated continuous monitoring program demonstrate progress towards a more robust implementation of the National Institute of Standards and Technology Special Publications 800-37, 800-39, 800-53, and 800-53A.

(U) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has approved and implemented a continuous monitoring policy that assesses the security state of information systems and is consistent with NIST Special Publications.

~~(SBU)~~ **Finding C. BBG Has Not Finalized and Implemented Contingency Plans**

~~(SBU)~~ We have reported deficiencies with BBG contingency plans since FY 2010. In FY 2014, we continue to find that BBG has not developed a policy for [Redacted] (b) (5) [Redacted] contingency plans. As a result, BBG has neither developed contingency plans nor performed any contingency testing in accordance with NIST guidelines.

(U) NIST SP 800-34, Revision 1,¹³ states that an organization should “develop a contingency planning policy statement, conduct a business impact analysis, identify preventive controls, create contingency strategies, develop an information system contingency plan, ensure plan testing, training, exercises, and ensure plan maintenance.” In addition, according to NIST SP 800-53, Revision 4,¹⁴ an organization should develop a contingency plan for the information system and coordinate contingency planning activities with incident handling activities.

~~(SBU)~~ According to BBG’s Director of Global Operations, the reason BBG has not developed a policy for [Redacted] (b) (5) [Redacted] contingency plans or performed contingency testing is because BBG embarked on a new emergency management and business continuity program designed to assess the various needs covering all aspects of its administration and operations. As a result, key policy documents covering contingency planning, business continuity, and disaster recovery were in draft form awaiting BBG management approval. However, without effective contingency plans, BBG may not be prepared to access or recover critical information and resources to perform mission critical business functions in the event of a disaster.

¹³ (U) NIST SP 800-34, rev. 1, *Contingency Planning Guide for Federal Information Systems*, “Executive Summary,” May 2010.

¹⁴ (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “CP-1 Contingency Planning Policy and Procedures,” April 2013 (last updated January 2014).

~~(SBU)~~ **Recommendation 6.** OIG recommends that the Broadcasting Board of Governors approve and implement a contingency plan policy for [Redacted] (b) (5) contingency plans, as required by the National Institute of Standards and Technology, Special Publication 800-34, Revision 1.

(U) Management Response: BBG concurred with this recommendation and stated the Agency is formalizing plans and policies related to Emergency Management and Business Continuity, including Crisis Communication and Management Succession plans and the Department of Homeland Security's Exercise and Evaluation Program to implement a performance-based, multi-year training and exercise program.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has approved and implemented a contingency plan policy for [Redacted] (b) (5) contingency plans, as required by NIST SP guidance.

~~(SBU)~~ **Recommendation 7.** OIG recommends that the Director of Global Operations complete and implement [Redacted] (b) (5) contingency plans for all information systems and conduct necessary testing as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 4.

(U) Management Response: BBG concurred with this recommendation and stated the Agency has embarked on a "Line of Business" Emergency Management and Business Continuity program designed to assess the various needs of departments covering all aspects of Agency administration and operations. Once completed, this material will be evaluated for acceptable levels of need and risk to become the framework for a complete overview of essential Agency requirements.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has completed and implemented [Redacted] (b) (5) contingency plans for all information systems and conduct necessary testing as required by NIST SP guidance.

(U) Finding D. BBG Has Not Implemented Effective Configuration Management Policies

(U) BBG has not effectively managed the configuration processes over its information systems since FY 2010. Specifically, BBG has not completed the development of procedures and guidance that govern routine and critical security configuration management processes. We identified the following deficiencies:

- **(U)** The Windows desktop and server configuration procedures did not contain all of the security settings from the U.S. Government Configuration Baseline in accordance with NIST SP 800-53, Revision 4.

- [Redacted] (b) (5) [Redacted]
- [Redacted] (b) (5) [Redacted]

(U) According to NIST SP 800-53, Revision 4,¹⁵ an organization should establish and document configuration settings for information technology products employed within its information systems using organization-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements; and identify, document, and approve any deviations from established configuration settings for organization-defined information system components based on organization-defined operational requirements.

(U) BBG’s IT Software Deployment Policy for Servers¹⁶ states that BBG will “test and disseminate Microsoft operating system and application patches released [Redacted] in a way that ensures complete coverage of servers while avoiding operational downtime by rigorously testing the patches prior to general release to ensure application compatibility and seamless functionality.”

(U) BBG’s Change Management Policy¹⁷ states, “To properly control changes, requests must be made formally to allow for thorough review as well as the updating of both systems and documentation,” and that “Requesters of non-emergency changes must assemble a complete set of change request documentation that must be reviewed and approved prior to non-emergency changes.”

(U) The deficiencies with configuration management occurred because:

- (U) BBG management believed that U.S. Government Configuration Baseline settings were adequately implemented in the Group Policy Object in Active Directory (AD), but we found that the server and desktop configuration procedures did not contain the settings described by management.

- [Redacted] (b) (5) [Redacted]

¹⁵ (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “CM-6 Configuration Settings,” April 2013 (last updated January 2014).

¹⁶ (U) *IT Software Deployment Policy for Servers*, “Objective,” December 2013.

¹⁷ (U) *Change Management Policy*, “Procedures,” November 2010.

[Redacted] (b) (5)

- (U) The change manager¹⁸ has overall responsibility for the change management process within the BBG IT department but failed to ensure that changes were fully documented and authorized.

(U) Without documented procedures that govern the performance of routine and critical processes, BBG IT systems are vulnerable to the denial of service, damage to the general support system that is the underlying system used throughout BBG to support applications, or the potential introduction of security attacks.

(U) Recommendation 8. OIG recommends that the Director of Global Operations update server and workstation baseline procedures to include all of the U.S. Government Configuration Baseline configuration settings as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Management Response: BBG did not concur with this recommendation. BBG welcomes an opportunity to demonstrate to the OIG that BBG successfully applied U.S. Government Configuration Baseline policies to computer objects through Group Policy Objects linked to BBG's Active Directory Organizational Units by using Microsoft's Resultant Set of Policy tool.

(U) OIG Reply: OIG considers the recommendation unresolved. OIG agrees that the Agency applied U.S. Government Configuration Baseline configuration settings to servers and workstations through Group Policy Objects. However, OIG determined that the Group Policy Objects were incomplete because they did not contain all available U.S. Government Configuration Baseline configuration settings. This recommendation can be closed when OIG receives and accepts documentation showing that all U.S. Government Configuration Baseline configuration settings are documented in server and workstation baseline procedures, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Recommendation 9. OIG recommends that the Director of Global Operations remediate all critical vulnerabilities as they are identified through periodic scanning.

(U) Management Response: BBG concurred with this recommendation and stated a continuous monitoring program is under development to proactively identify and remediate security vulnerabilities caused by inadequate patch verification and poor software version control.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has remediated all critical vulnerabilities as they are identified through periodic scanning.

¹⁸ (U) As defined in BBG's *Change Management Policy*.

(U) **Recommendation 10.** OIG recommends that the Director of Global Operations enforce the Broadcasting Board of Governors (BBG) Change Management Policy for all changes within the BBG environment.

(U) **Management Response:** BBG concurred with this recommendation and stated the Chief Information Officer has taken steps to ensure that the BBG's Change Management program more fully aligns with its policy. When feasible, all changes to BBG's IT systems will be tested and authorized before implementation.

(U) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency appropriately authorizes, tests, and approves all changes within the BBG environment in accordance with the BBG Change Management Policy.

(U) Finding E. BBG Has Not Implemented an Effective Incident Response and Reporting Program

(U) OIG has reported BBG security incident program deficiencies since FY 2010. In FY 2014, BBG still has not implemented an effective incident response and reporting program. Specifically, BBG's standard operating procedures for the Computer Security Incident Response Team has not implemented the preparation, detection and analysis, containment, eradication, recovery, and post-incident activity components into their incident response life cycle, as required by NIST SP 800-61, Revision 2.

(U) NIST SP 800-61, Revision 2,¹⁹ states that establishing an incident response capability should include the following actions:

- (U) Creating an incident response policy and plan;
- (U) Developing procedures for performing incident handling and reporting;
- (U) Setting guidelines for communicating with outside parties regarding incidents;
- (U) Selecting a team structure and staffing model;
- (U) Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies);
- (U) Determining what services the incident response team should provide.

(U) In addition, 6 of 11 (55 percent) incidents for FY 2014 do not have an assigned categorization level as required by BBG's *Computer Security Incident Management Policy*,²⁰ which states:

¹⁹ (U) NIST SP 800-61, rev. 2, *Computer Security Incident Handling Guide*, "Executive Summary," August 2012.

²⁰ (U) Computer Security Incident Management Policy, "Computer Security Incident Response Procedures," May 2011 (last updated January 2012).

(U) The CSIRT [Computer Security Incident Response Team] team will first categorize, per US-CERT's standards (NIST SP 800-61), the incident and open an incident tracking ticket. Following this action, they will initially assess the incident to determine (if possible) whether its origin is external or internal to the agency, the scope, status (ongoing or contained), impact to the agency's mission, and/or impact on employee or contractor PII [Personally Identifiable Information] data. Depending on the incident's categorization and impact, it may be reported to US-CERT, FBI and the agency's senior management team, per the following escalation matrix.

(U) In FY 2013, BBG recognized the weakness in its incident response and reporting policy and drafted a new *Computer Security Incident Management Policy* in FY 2014 that is currently undergoing management review and approval. However, at the time of our fieldwork, the policy had not been approved and implemented. In addition, although BBG drafted the policy, the Information Security Management Division has not provided sufficient incident management procedures for staff to adhere to because the division thought the current policy and standard operating procedures were adequate (contained sufficient details) for daily operations. These procedures are important because they provide staff with sufficient details to perform their daily duties to identify and respond to incidents that could degrade BBG's information systems. Without an effective incident response and reporting policy and procedures, a shutdown of BBG information systems could occur, impacting its operational mission.

(U) Recommendation 11. OIG recommends that the Information Security Management Division update and implement the incident response policy and procedures to include preparation, detection and analysis, containment, eradication, recovery, and post-incident activity components as required by National Institute of Standards and Technology Special Publication 800-61, Revision 2.

(U) Management Response: BBG concurred with this recommendation and stated the Agency recently drafted a new Computer Security Incident Management Policy that is compliant with NIST SP 800-61, Revision 2. The policy is undergoing review to ensure compatibility with the unique issues of the Agency's newsgathering, production, and content distribution activities.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has updated and implemented the incident response policy and procedures to include preparation, detection and analysis, containment, eradication, recovery, and post-incident activity components as required by NIST SP 800-61, Revision 2.

(U) Recommendation 12. OIG recommends that the Information Security Management Division adhere to the *Computer Security Incident Management Policy*, when finalized, to include the appropriate category level for every documented incident.

(U) Management Response: BBG concurred with this recommendation and stated the Agency's Information Security Management Division will develop procedures to ensure compliance with its Computer Security Incident Management Policy.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has adhered to the finalized *Computer Security Incident Management Policy*, to include the appropriate category level for every documented incident.

(U) Finding F. BBG Has Not Fully Followed Its Plans of Action and Milestones Policy

(U) We have identified POA&M deficiencies in BBG's information security process since FY 2010. In FY 2014, we found that BBG's system owners, in coordination with the Office of the Chief Information Officer, have not adhered to BBG's process of completing all the necessary elements of a POA&M, as stated in the *Information Security POA&M Policy*.²¹ For all six of the systems in our target population that we tested, we found that the POA&Ms, in the POA&M database, have not consistently provided sufficient detail such as the severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the latest status.

(U) The weakness with the POA&M process occurred because the Chief Information Security Officer, under the guidance of the Director of Global Operations, failed to fully carry out responsibilities to coordinate and manage the POA&M process with system owners. In addition, according to a BBG official, system owners did not believe all the POA&M elements were required to be documented due to the small size of the agency.

(U) Without adequate identification, assessment, prioritization, and monitoring of corrective actions on an enterprise basis, the most important actions (highest security risks) related to BBG's information security program may not be fully funded or resolved in a timely manner, thus exposing BBG's sensitive data, systems, and hardware to unauthorized access and activities.

(U) Recommendation 13. OIG recommends that the Chief Information Security Officer, in coordination with the system owners and the Office of the Chief Information Officer, ensure that Broadcasting Board of Governors' Plans of Action and Milestones (POA&M) include all required elements in accordance with the *Information Security POA&M Policy*, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the latest status.

(U) Management Response: BBG concurred with this recommendation and stated the Agency will work to incorporate more POA&M details for all active issues being remediated during FY 2015.

²¹ (U) *Information Security Plan of Action and Milestones (POA&M) Policy*, "Policy Provisions," May 2010.

(U) **OIG Reply:** OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has included all required elements in accordance with the *Information Security POA&M Policy*, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the latest status.

(U) Finding G. BBG's Remote Access Controls Can Be Improved

(U) We found that BBG has not implemented procedures to ensure remote access policies and guidance, such as BBG's Virtual Private Network (VPN) Access Acceptance Form and NIST SP 800-53, Revision 4, were followed. The Enterprise Networks and Storage Division has not implemented procedures to ensure that remote access was granted only to computers that had security safeguards that complied with BBG's policies and procedures. This condition occurred even though BBG purchased a system in FY 2013 to enforce remote access policies and procedures. However, BBG has not fully implemented the system as part of its major infrastructure change. As of FY 2014, BBG has completed the proof of concept for the system build and system build acceptance testing, but has not yet implemented the solution into production. Further, the Enterprise Networks and Storage Division did not disable one of two VPN tokens that were reported lost. This occurred because the Enterprise Networks and Storage Division had only one administrator that possessed the knowledge of how to disable lost tokens and that administrator was unavailable to disable the token at the time the token was reported lost.

(U) According to BBG's VPN Access Acceptance Form, users' computers must be configured to comply with BBG security requirements, including using up-to-date virus scan and virus definitions. In regards to disabling lost tokens, NIST SP 800-53, Revision 4,²² states:

(U) Specific actions that can be taken to safeguard authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing individual authenticators with others, and reporting lost, stolen, or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance.

(U) By not implementing procedures that require the use of properly secured computers and remote access tokens, BBG may be unable to ensure the security of its data and network. The risks of introducing viruses, worms, or other malicious code into BBG's network are increased significantly, which could result in a loss of data and/or compromise of BBG's systems.

²² (U) NIST SP 800-53, rev. 4, "Security and Privacy Controls for Federal Information Systems and Organizations," "IA-5 Authenticator Management," April 2013 (last updated January 2014).

(U) Recommendation 14. OIG recommends that the Enterprise Networks and Storage Division implement procedures to assess the adequacy of the security configurations of remote computers that request access to the Broadcasting Board of Governors' (BBG) network and grant access only to properly configured and patched devices, as required by BBG's Virtual Private Network (VPN) policy and VPN Access Acceptance Form.

(U) Management Response: BBG concurred with this recommendation and stated the Agency has recently completed several "Proof of Concepts" to address this weakness. Subject to available funding, the Agency intends to deploy them across all elements of BBG's Washington Network during FY 2015.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has implemented procedures to assess the adequacy of the security configurations of remote computers that request access to the BBG network and grant access only to properly configured and patched devices, as required by BBG's VPN policy and VPN Access Acceptance Form.

(U) Recommendation 15. OIG recommends that the Enterprise Networks and Storage Division ensure that multiple personnel are trained, and utilize that training, to disable Virtual Private Network tokens after they are reported lost or stolen in accordance with National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

(U) Management Response: BBG concurred with this recommendation and stated the Agency will ensure that multiple Customer Systems Support Division staff members are trained and follow consistent procedures when they issue and disable remote access tokens during FY 2015.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that the Agency has ensured that multiple personnel are trained, and utilize that training, to disable Virtual Private Network tokens after they are reported lost or stolen in accordance with NIST SP 800-53, Revision 4.

(U) Finding H. BBG Has Not Implemented Effective Identity and Access Management Practices

(U) We have reported annually since FY 2010 that BBG has not implemented Personal Identity Verification (PIV) cards and deficiencies exist with user account management that impact BBG's information security program. In FY 2014, these weaknesses continue to be identified. Specifically, as of February 2014, BBG employees and contractors have been issued 69 of 2,223 (3 percent) PIV cards,²³ while the expected level of compliance for the OMB

²³ (U) Although PIV cards were issued, BBG was not utilizing them for physical or logical access capabilities.

required use of PIV cards for user authentication was 75 percent in FY 2014.²⁴ In addition, we continued to identify user account management control weaknesses in FY 2014 that collectively could result in the submission of false transactions, improper access, and dissemination of confidential data or other malicious activities. Specifically, we found the following weaknesses:

[Redacted] (b) (5)

(U) Homeland Security Presidential Directive 12²⁵ mandates a Federal standard for secure and reliable forms of identification. The directive states that the heads of Executive departments and agencies should “require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems.”

(U) BBG’s *Identification and Authentication Policy*²⁶ states that system owners are responsible for implementing the policy and procedures for their IT systems, including:

- (U) monitoring and taking actions to create and delete accounts;
- (U) creating processes to disable user IDs that have been inactive for 45 or more days;
- (U) creating processes to disable separating/terminating user accounts within 24 hours of notification, and removing these disabled accounts within a week of notification, unless the Security Manager determines that removing the disabled account would adversely affect operations;
- (U) creating processes to review the use of guest, test, and shared accounts, and report such accounts quarterly with their justification to the Chief Information Security Officer. Unneeded accounts shall be disabled and/or deleted whenever possible.

(U) The weaknesses identified with the PIV cards occurred because the Office of Security purchased a Commercial Off-the-Shelf product in 2006 that was not compatible with BBG’s legacy security system until adjustments were made in March 2013. In addition, a BBG official explained that FY 2014 budget constraints delayed implementation of PIV cards and

²⁴ (U) DHS, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, “Expected Levels of Performance,” December 2013.

²⁵ (U) *Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors*, August 2004.

²⁶ (U) *Identification and Authentication Policy*, “Policy Provisions,” April 2011 (last updated March 2012).

BBG intended to accelerate the issuance of PIV cards as much as practical within their budget constraints. With respect to user account management, BBG was in the process of restructuring its AD Organizational Units, and the automated script utilized to monitor user account compliance with BBG's *Identification and Authentication Policy* had not been modified to detect non-compliant user accounts within the new Organizational Units. As a result, the automated script did not detect non-compliant user accounts. Non-compliant user accounts could be utilized to submit false transactions, grant further improper access, and disseminate confidential data or other malicious activities.

(U) Recommendation 16. OIG recommends that the Director of Global Operations and system owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors' *Identification and Authentication Policy*.

(U) Management Response: BBG concurred with this recommendation and stated a continuous monitoring program is under development to ensure that authorization and access control is consistently enforced on all domain and local user accounts in accordance with the BBG's user account configuration policy.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that user accounts are properly maintained in accordance with Broadcasting Board of Governors' *Identification and Authentication Policy*.

(U) Recommendation 17. OIG recommends that the Director of Global Operations, in coordination with the Office of Security, complete the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12 and Office of Management and Budget guidelines.

(U) Management Response: BBG concurred with this recommendation and stated the Agency has accelerated issuance of PIV cards to its employees and contractors in 2014 and will continue to issue cards at this pace in 2015. In addition, the Chief Information Officer will continue to assess progress on PIV issuance and expand its usage as part of logical access control within the BBG's network as much as practical within the budget constraints imposed on the Agency.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing the completion of issuance of PIV cards as required by Homeland Security Presidential Directive 12 and Office of Management and Budget guidelines.

(U) Finding I. BBG's Security Training Policy Did Not Contain Role-Based Training

(U) We found that key IT personnel with security responsibilities have not completed role-based security training. Role-based security training addresses technology changes or patterns of vulnerabilities in information systems for individuals with significant IT security

responsibilities. NIST SP 800-53, Revision 4,²⁷ states that the “organization provides role-based security-related training before authorizing access to the system.”

(U) According to a BBG official, the Agency drafted a revised security training policy that included the Chief Information Security Officer’s responsibility for creating content, administering the training, and tracking compliance with role-based training. However, BBG’s Director of Global Operations has not finalized or implemented the revised overall security training policy.

(U) Without the completion of role-based security training, key IT personnel may not fully understand their security responsibilities and the methods and techniques used to protect the network from attackers.

(U) Recommendation 18. OIG recommends that the Director of Global Operations finalize and implement a role-based security training policy, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Management Response: BBG concurred with this recommendation and stated the Chief Information Officer will take steps to develop and implement a role-based IT security program, within budgetary limitations, in accordance with guidance from the National Institute of Standards and Technology, during FY 2015.

(U) OIG Reply: OIG considers the recommendation resolved. This recommendation can be closed when OIG receives and accepts documentation showing that a role-based security training policy was finalized and implemented, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Finding J. BBG Has Complied with Contractor Oversight and Security Capital Planning Requirements

(U) In FY 2014, we found that BBG was in compliance with the contractor oversight and security capital planning requirements. There were no prior year weaknesses that carried over to FY 2014 for these two areas.

(U) For contractor oversight, BBG has established a program to oversee systems operated on its behalf by contractors or other entities, including organization systems and services residing in the cloud external to BBG.

(U) For security capital planning, there have been no major IT investments or capital investments funding in FY 2014. However, OIG suggests the Director of Global Operations, in coordination with the Deputy Chief Information Officer, implement processes and procedures to cross-reference POA&M information, including costs, to the capital planning budget process with a Unique Investment Identifier for any future IT acquisitions.

²⁷ (U) NIST SP 800-53, rev. 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, “AT-3 Role-Based Security Training,” April 2013 (last updated January 2014).

(U) List of Recommendations

(U) Recommendation 1. OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Office of Cuba Broadcasting Headquarters Network system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) Recommendation 2. OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Privacy Information Enclave system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) Recommendation 3. OIG recommends that the Broadcasting Board of Governors update the Certification and Accreditation Policy and Procedures to identify the responsible organizations for conducting annual security control assessments.

(U) Recommendation 4. OIG recommends that the Broadcasting Board of Governors perform annual security control assessments on its Identity Management System.

(U) Recommendation 5. OIG recommends that the Director of Global Operations approve and implement a continuous monitoring policy that assesses the security state of information systems and is consistent with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

~~(SBU)~~ **Recommendation 6.** OIG recommends that the Broadcasting Board of Governors approve and implement a contingency plan policy for [REDACTED] contingency plans, as required by the National Institute of Standards and Technology, Special Publication 800-34, Revision 1.

~~(SBU)~~ **Recommendation 7.** OIG recommends that the Director of Global Operations complete and implement [Redacted] (b) (5) contingency plans for all information systems and conduct necessary testing as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 4.

(U) Recommendation 8. OIG recommends that the Director of Global Operations update server and workstation baseline procedures to include all of the U.S. Government Configuration Baseline configuration settings as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Recommendation 9. OIG recommends that the Director of Global Operations remediate all critical vulnerabilities as they are identified through periodic scanning.

(U) Recommendation 10. OIG recommends that the Director of Global Operations enforce the Broadcasting Board of Governors (BBG) Change Management Policy for all changes within the BBG environment.

(U) Recommendation 11. OIG recommends that the Information Security Management Division update and implement the incident response policy and procedures to include preparation, detection and analysis, containment, eradication, recovery, and post-incident activity components as required by National Institute of Standards and Technology Special Publication 800-61, Revision 2.

(U) Recommendation 12. OIG recommends that the Information Security Management Division adhere to the *Computer Security Incident Management Policy*, when finalized, to include the appropriate category level for every documented incident.

(U) Recommendation 13. OIG recommends that the Director of Global Operations, in coordination with the system owners and the Office of the Chief Information Officer, ensure that Broadcasting Board of Governors' Plans of Action and Milestones (POA&M) include all required elements in accordance with the *Information Security POA&M Policy*, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the latest status.

(U) Recommendation 14. OIG recommends that the Enterprise Networks and Storage Division implement procedures to assess the adequacy of the security configurations of remote computers that request access to the Broadcasting Board of Governors' (BBG) network and grant access only to properly configured and patched devices, as required by BBG's Virtual Private Network (VPN) policy and VPN Access Acceptance Form.

(U) Recommendation 15. OIG recommends that the Enterprise Networks and Storage Division ensure that multiple personnel are trained, and utilize that training, to disable Virtual Private Network tokens after they are reported lost or stolen in accordance with National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

(U) Recommendation 16. OIG recommends that the Director of Global Operations and system owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors' *Identification and Authentication Policy*.

(U) Recommendation 17. OIG recommends that the Director of Global Operations, in coordination with the Office of Security, complete the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12 and Office of Management and Budget guidelines.

(U) Recommendation 18. OIG recommends that the Director of Global Operations finalize and implement a role-based security training policy, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) Scope and Methodology

(U) In order to fulfill its responsibilities related to the Federal Information Security Management Act of 2002 (FISMA),¹ the Office of Inspector General (OIG), Office of Audits, contracted with Williams, Adley & Company-DC, LLP (referred to as “we” in this appendix), an independent public accountant, to evaluate the Broadcasting Board of Governors’ (BBG) information security program and practices to determine the effectiveness of such programs and practices for FY 2014.

(U) FISMA requires each Federal agency to develop, document, and implement an agency-wide program to provide information security for the information systems that support the operations and assets of the agency, including those provided or managed by another agency or contractor or another source. To ensure the adequacy and effectiveness of these controls, FISMA requires the agency inspector general or an independent external auditor to perform annual reviews of the information security program and to report those results to the Office of Management and Budget (OMB) and the Department of Homeland Security (DHS).² DHS uses this data to assist in oversight responsibilities and to prepare its annual report to Congress regarding agency compliance with FISMA.

(U) We conducted the audit work from April through July 2014. In addition, we performed the audit in accordance with Generally Accepted Government Auditing Standards, FISMA, OMB, and National Institute of Standards and Technology (NIST) guidance. Generally Accepted Government Auditing Standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We and OIG believe that the evidence obtained provides a reasonable basis for the findings and conclusions based on the audit objectives.

(U) We used the following laws, regulations, and policies to evaluate the adequacy of the controls in place at BBG:

- (U) DHS Inspector General FISMA Reporting Metrics.³
- (U) OMB Memoranda M-02-01, M-04-04, M-06-19, and M-12-20.⁴

¹ (U) Pub. L. No. 107-347, tit. III, 116 Stat. 2946 (2002).

² (U) OMB Memorandum M-10-28, *Clarifying Cybersecurity Responsibilities and Activities of the Executive Office of the President and Department of Homeland Security (DHS)*, July 6, 2010.

³ (U) DHS, *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, December 2013.

⁴ (U) OMB Memorandum M-02-01, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, October 2001; OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, December 2003; OMB Memorandum M-06-19, *Reporting Incidents Involving Personally Identifiable Information and Incorporating the Cost for Security in Agency Information Technology Investments*, July 2006; OMB Memorandum M-12-20, *FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, September 2012.

- (U) BBG policies and procedures, such as BBG's *Computer Security Incident Management Policy*.
- (U) Federal laws, regulations, and standards, such as FISMA and those contained in OMB Circular No. A-130, Revised,⁵ and OMB Circular No. A-11.⁶
- (U) NIST Special Publications, Federal Information Processing Standards Publications, other applicable NIST publications, and industry best practices.

(U) During our audit, we assessed BBG's information security program policies, procedures, and processes in the following areas:

- (U) Continuous monitoring management
- (U) Configuration management
- (U) Identity and access management
- (U) Incident response and reporting
- (U) Risk management
- (U) Security training
- (U) Plans of action and milestones (POA&M)
- (U) Remote access management
- (U) Contingency planning
- (U) Contractor oversight
- (U) Security capital planning

(U) The audit covered the period October 1, 2013, to July 31, 2014. During audit fieldwork, we took the following actions:

- (U) Determined the extent to which the BBG's information security plans, programs, and practices complied with FISMA requirements; applicable Federal laws, regulations, and standards; relevant OMB Circular No. A-130, revised processes and reporting requirements included in Appendix III; and NIST and Federal Information Processing Standards Publications requirements.
- (U) Reviewed relevant security programs and practices to report on the effectiveness of BBG's Agency-wide information security program in accordance with OMB's annual FISMA reporting instructions. The audit approach addressed the DHS *FY 2014 Inspector General Federal Information Security Management Act Reporting Metrics*, dated December 2, 2013.
- (U) Assessed programs for monitoring of security policy and program compliance and responding to security events, e.g., unauthorized changes detected by intrusion detection systems.
- (U) Assessed the adequacy of internal controls related to the areas reviewed.

⁵ (U) OMB Circular No. A-130, Revised, *Management of Federal Information Resources*, "Security of Federal Automated Information Resources," November 2000.

⁶ (U) OMB Circular No. A-11, *Preparation, Submission, and Execution of the Budget*, August 2011.

Control deficiencies OIG identified are presented in the Audit Results section of this report.

- (U) Evaluated BBG's remedial actions taken to address the previously reported information security program control weaknesses identified in OIG's *Audit of the Broadcasting Board of Governors Information Security Program* (AUD-IT-IB-14-02, Oct. 2013).

(U) Review of Internal Controls

(U) We reviewed BBG's internal controls to determine whether:

- (U) The Agency has established and maintained an enterprise-wide continuous monitoring program that assessed the security state of information systems that were consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Agency has established and maintained a security configuration management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Agency has established and maintained an identity and access management program that was generally consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and that identified users and network devices.
- (U) The Agency has established and maintained an incident response and reporting program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Agency has established and maintained a risk management program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Agency has established and maintained a security training program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines.
- (U) The Agency has established and maintained a POA&M program that was consistent with FISMA requirements, OMB policy, and applicable NIST guidelines and tracked and monitored known information security weaknesses.
- (U) The Agency has established and maintained a remote access program that was generally consistent with NIST and OMB FISMA requirements.
- (U) The Agency has established and maintained an entity-wide business continuity and disaster recovery program that was generally consistent with NIST and OMB FISMA requirements.
- (U) The Agency has established and maintained a program to oversee systems operated on its behalf by contractors or other entities, including Agency systems and services residing in the cloud external to the Agency.
- (U) The Agency has established and maintained a capital planning and investment program for information security.

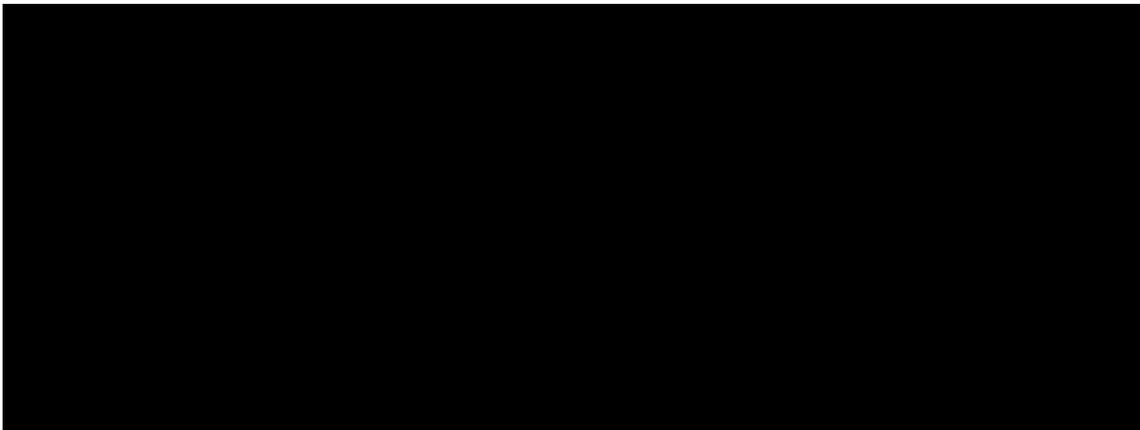
(U) On October 14, 2014, OIG held an exit conference to present all findings identified during the audit with BBG management. Deficiencies identified with BBG's internal controls are presented in the Audit Results section of this report.

(U) Use of Computer-Processed Data

(U) During the audit, we utilized computer-processed data to obtain samples and information regarding the existence of information security controls. Specifically, we obtained data extracted from Microsoft's Windows Active Directory and BBG's human resources system to test user account management controls. We assessed the reliability of computer-generated data primarily by comparing selected data with source documents. We determined that the information was sufficiently reliable for assessing the adequacy of related information security controls.

(U) Sampling Methodology

(U) We received a population of six FISMA reportable systems for which an Authority to Operate was conducted within the last 3 years. We tested all six systems in our target population indicated below (see Table 1).



(U) *Government Auditing Standards* indicate that either a statistical or judgment sample can yield sufficient and appropriate audit evidence. A statistical sample is generally preferable, although it may not always be practicable. By definition, a statistical sample requires that each sampling unit in the population be selected via a random process and have a known, non-zero chance of selection. These requirements often pose a problem when conducting audits within BBG. All information systems, irrespective of size, must have a chance to be randomly selected. Therefore, the exclusion of one or more systems cannot be allowed. In other words, all systems—large and small—must have a chance to be randomly selected, and that chance must not be zero. However, BBG would undoubtedly deem many systems too small and atypical to merit inclusion in an OIG sample.

(U) Consequently, we employed another type of sample permitted by *Government Auditing Standards*—namely, a non-statistical sample known as a judgment sample. A judgment sample is a sample selected by using discretionary criteria rather than criteria based on the laws

of probability. As in this audit, we and OIG routinely take great care in determining the criteria to use for sampling systems, and other population sampling units. Moreover, we used, whenever practicable, random numbers to preclude the introduction of any bias in sample selection although a non-statistical technique was utilized. We acknowledge that it is possible that the information security deficiencies identified in this report may not be as prevalent or may not exist in all systems that we have not tested. However, a prudent person without any basis in fact would not automatically assume that these conditions are non-existent in other systems. Such a supposition would be especially ill-advised for an issue as important as information security.

(U) Where we deemed it was appropriate, we used audit sampling techniques to perform audit procedures to less than 100 percent of the population to enable us to evaluate audit evidence of the items selected to assist in forming a conclusion concerning the population. Generally, for a large population of sample items (more than 2,000) and frequent operating controls (that is, daily operating controls), we used non-statistical sampling methods to test 22 items.⁷ However, for small populations (less than 2,000) and infrequent operating controls, we used the following table as guidance to select sample sizes (see Table 2).

(U) Table 2. Small Population Size*

Control Frequency	Sample Size
Quarterly (4)	2
Monthly (12)	2
Semimonthly (24)	3
Weekly (52)	5

* (U) *AICPA Audit Guide*, “Small Populations and Infrequently Operating Controls Table 3-5,” March 2012.

⁷ (U) *AICPA Audit Guide*, “AAG-SAM Appendix A,” March 2012.

(U) Followup of Recommendations from the FY 2013 Audit of the Broadcasting Board of Governors Information Security Program

(U) The audit team reviewed actions implemented by management to mitigate the findings identified in the FY 2013 audit of the Broadcasting Board of Governors (BBG) information security program. The current status of each of the recommendations follows:

(U) Recommendation 1. OIG recommends that the System Owners, Information Owners, and the Chief Information Officer/Chief Technology Officer assess the data categorization for information systems, in accordance with Federal Information Processing Standard 199, and implement the corresponding National Institute of Standards and Technology Special Publication 800-53, Revision 3, controls, if necessary.

(U) Status: Closed. System owners, information owners, and the Director of Global Operations reassessed the data categorization for BBG information systems, in accordance with Federal Information Processing Standard 199, and implemented the corresponding National Institute of Standards and Technology Special Publication 800-53 controls.

(U) Recommendation 2. OIG recommends that the System Owners and Chief Information Officer/Chief Technology Officer prioritize resources to perform security impact analyses to assess the differences in National Institute of Standards and Technology Special Publication 800-53, Revision 3, control families and their impact to the state of security on the systems and reauthorize the systems.

(U) Status: Closed. BBG performed security impact analyses on their information systems to assess the differences in National Institute of Standards and Technology Special Publication 800-53, Revision 3, control families and their impact to the state of security on the systems and reauthorize the systems.

(U) Recommendation 3. OIG recommends that the Broadcasting Board of Governors prioritize resources to perform a privacy impact assessment for the Privacy Information Enclave in accordance with Office of Management and Budget Memorandum M-12-20.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 1 (Finding A) in the FY 2014 report.

(U) Recommendation 4. OIG recommends that the Chief Information Officer/Chief Technology Officer, in coordination with the Information Security Management Division, finalize and implement an enterprise-wide continuous monitoring strategy that includes a continuous monitoring policy and assesses the security state of information systems in a manner consistent with Federal Information Security Management Act requirements, Office of Management and Budget policy, and applicable National Institute of Standards and Technology guidelines.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 5 (Finding B) in the FY 2014 report.

(U) Recommendation 5. OIG recommends that the Chief Information Officer/Chief Technology Officer prioritize resources to complete **[Redacted] (b) (5)** contingency planning documents for all information systems, and conduct necessary testing in accordance with National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 3.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 6 (Finding C) in the FY 2014 report.

(U) Recommendation 6. OIG recommends that the Information Security Management Division update and implement its incident response policy in accordance with National Institute of Standards and Technology Special Publication 800-61, Revision 2.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 11 (Finding E) in the FY 2014 report.

(U) Recommendation 7. OIG recommends the Chief Information Officer/Chief Technology Officer ensure that Broadcasting Board of Governors Plans of Action and Milestones (POA&M) include all required elements in accordance with its Information Security POA&M Policy, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the status.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 13 (Finding F) in the FY 2014 report.

(U) Recommendation 8. OIG recommends that the Enterprise Networks and Storage Division, under the Office of the Chief Information Officer/Chief Technology Officer, implement procedures to assess the adequacy of the security configurations of mobile computers that request access to the Broadcasting Board of Governors network and grant access only to properly configured and patched devices in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 14 (Finding G) in the FY 2014 report.

(U) Recommendation 9. OIG recommends that the Chief Information Officer/Chief Technology Officer verify that U.S. Government Configuration Baseline configuration standards are implemented and compliance with the implemented standards is periodically assessed in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 8 (Finding D) in the FY 2014 report.

(U) Recommendation 10. OIG recommends that the Chief Information Officer/Chief Technology Officer follow the Broadcasting Board of Governors (BBG) Change Management Policy, to “test and disseminate Microsoft operating system and application patches released [Redacted] (b) (5) in a way that ensures complete coverage of workstations and laptops while avoiding operational downtime by rigorously testing the patches prior to general release to ensure application compatibility and seamless functionality.”

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 10 (Finding D) in the FY 2014 report.

(U) Recommendation 11. OIG recommends that the Chief Information Officer/Chief Technology Officer and system owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors (BBG) Identification and Authentication Policy and the BBG/IBB/VOA Password Policy.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 16 (Finding H) in the FY 2014 report.

(U) Recommendation 12. OIG recommends that the Office of Security, in coordination with the Chief Information Officer/Chief Technology Officer, complete the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 17 (Finding H) in the FY 2014 report.

(U) Recommendation 13. OIG recommends that the Information Security Management Division, in coordination with the Chief Information Officer/Chief Technology Officer, prioritize resources to develop and implement a role-based security training program in accordance with National Institute of Standards and Technology Special Publication 800-53, Revision 3.

(U) Status: Closed from FY 2013 report; this repeat recommendation has become Recommendation 18 (Finding I) in the FY 2014 report.

(U) Appendix C

(U) Broadcasting Board of Governors Response

Broadcasting Board of Governors
INTERNATIONAL BROADCASTING BUREAU

October 17, 2014

Mr. Norman P. Brown
Assistant Inspector General
for Audits
Office of Inspector General
U.S. Department of State

Dear Mr. Brown:

Enclosed is the response to the Office of Inspector General (OIG) draft report, "Audit of the Broadcasting Board of Governors Information Security Program," AUD-IT-IB-XX-XX, October 2014.

The Broadcasting Board of Governors (BBG) has reviewed the draft report and appreciates the opportunity to address the report's 18 recommendations as provided in the enclosure. BBG Director of Global Operations, Andre Mendes, has cleared/approved the Agency response to the recommendations in the draft OIG report.

Enclosure

330 Independence Avenue, SW

Washington, DC 20237

Enclosure

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

**BBG's Response to OIG's Draft "Audit of the Broadcasting Board of Governors
Information Security Program,"
Report Number AUD-IT-IB-14-XX, October 2014**
~~Sensitive but Unclassified~~

(U) Recommendation 1. OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Office of Cuba Broadcasting Headquarters Network system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) BBG Response (October 17, 2014): BBG concurs. The Agency will perform a privacy impact assessment for the Office of Cuba Broadcasting FISMA domain during FY 2015.

(U) Recommendation 2. OIG recommends that the Broadcasting Board of Governors perform a privacy impact assessment for its Privacy Information Enclave system, as required by National Institute of Standards and Technology Special Publication 800-37, Revision 1.

(U) BBG Response (October 17, 2014): BBG concurs. The Agency will perform a privacy impact assessment for the Privacy Information Enclave FISMA domain during FY 2015.

(U) Recommendation 3. OIG recommends that the Broadcasting Board of Governors update the Certification and Accreditation Policy and Procedures to identify the responsible organizations for conducting annual security control assessments.

(U) BBG Response (October 17, 2014): BBG concurs. The CIO will prioritize resources to ensure the Certification and Accreditation Policy and Procedures with the associated tracking sheets appropriately identify all responsible parties.

(U) Recommendation 4. OIG recommends that the Broadcasting Board of Governors perform annual security control assessments on its Identity Management System.

(U) BBG Response (October 17, 2014): BBG concurs. The BBG will work to complete all the required annual FISMA security reassessments during FY 2015 as the Agency adopts the Risk Management Framework in the National Institute of Standards and Technology (NIST) SP 800-53, Revision 4.

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

(U) Recommendation 5. OIG recommends that the Director of Global Operations approve and implement a continuous monitoring policy that assesses the security state of information systems and is consistent with National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) BBG Response (October 17, 2014): BBG concurs. The CIO will continue to ensure that the continuous monitoring policy and the associated continuous monitoring program at BBG demonstrate progress towards a more robust implementation of the NIST standards 800-137, 39, 53, and 53A.

(SBU) Recommendation 6. OIG recommends that the Broadcasting Board of Governors approve and implement a contingency plan policy for [REDACTED] and [REDACTED] contingency plans, as required by the National Institute of Standards and Technology, Special Publication 800-34, Revision 1.

(SBU) BBG Response (October 17, 2014): BBG concurs. The Agency is formalizing plans and policies related to Emergency Management and Business Continuity, including Crisis Communication and Management Succession plans and a multi-year Test, Training, and Exercise Program. This multi-year program and plan uses the Homeland Security Exercise and Evaluation Program (HSEEP) doctrine of the Department of Homeland Security to implement an “All-Hazards” and performance-based, multi-year training and exercise program.

(SBU) Recommendation 7. OIG recommends that the Director of Global Operations complete and implement system-specific and entity-wide contingency plans for all information systems and conduct necessary testing as required by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-34, Revision 1, and NIST SP 800-53, Revision 4.

(SBU) BBG Response (October 17, 2014): BBG concurs. The Agency has embarked on a “Line of Business” Emergency Management and Business Continuity program designed to assess the various needs of departments covering all aspects of Agency administration and operations. Once completed, this material will be evaluated for acceptable levels of need and risk to become the framework for a complete overview of essential Agency requirements.

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

(U) Recommendation 8. OIG recommends that the Director of Global Operations update server and workstation baseline procedures to include all of the U.S. Government Configuration Baseline configuration settings as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) BBG Response (October 17, 2014): BBG does not concur. The BBG welcomes an opportunity to demonstrate to the OIG auditors that the BBG successfully applies U.S. Government Configuration Baseline policies to computer objects through Group Policy Objects linked to the BBG's Active Directory Organizational Units by using Microsoft's Resultant Set of Policy tool.

(U) Recommendation 9. OIG recommends that the Director of Global Operations remediate all critical vulnerabilities as they are identified through periodic scanning.

(U) BBG Response (October 17, 2014): BBG concurs. A continuous monitoring program is under development to proactively identify and remediate security vulnerabilities caused by inadequate patch verification and poor software version control.

(U) Recommendation 10. OIG recommends that the Director of Global Operations enforce the Broadcasting Board of Governors (BBG) Change Management Policy for all changes within the BBG environment.

(U) BBG Response (October 17, 2014): BBG concurs. The CIO has taken steps to ensure that the BBG's Change Management program more fully aligns with BBG's policy. When feasible, all changes to BBG's IT systems will be tested and authorized before implementation.

(U) Recommendation 11. OIG recommends that the Information Security Management Division update and implement the incident response policy and procedures to include preparation, detection and analysis, containment, eradication, recovery, and post-incident activity components as required by National Institute of Standards and Technology Special Publication 800-61, Revision 2.

(U) BBG Response (October 17, 2014): BBG concurs. The Agency recently drafted a new Computer Security Incident Management Policy that is compliant with NIST SP 800-61, Revision 2. The policy is undergoing review to ensure compatibility with the unique issues of the Agency's newsgathering, production, and content distribution activities.

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

(U) Recommendation 12. OIG recommends that the Information Security Management Division adhere to the *Computer Security Incident Management Policy*, when finalized, to include the appropriate category level for every documented incident.

(U) BBG Response (October 17, 2014): BBG concurs. **The Agency's Information Security Management Division will develop procedures to ensure compliance with its Computer Security Incident Management Policy.**

(U) Recommendation 13. OIG recommends that the Chief Information Security Officer, in coordination with the system owners and the Office of the Chief Information Officer, ensure that Broadcasting Board of Governors' Plans of Action and Milestones (POA&M) include all required elements in accordance with the *Information Security POA&M Policy*, to include severity of the weakness, responsible organization, estimated funding resources, completion date, key milestones and changes, source of the weakness, and the latest status.

(U) BBG Response (October 17, 2014): BBG concurs. **The BBG will work to incorporate more POA&M details for all active issues being remediated during FY 2015 within its FISMA POA&M documentation.**

(U) Recommendation 14. OIG recommends that the Enterprise Networks and Storage Division implement procedures to assess the adequacy of the security configurations of remote computers that request access to the Broadcasting Board of Governors' (BBG) network and grant access only to properly configured and patched devices, as required by BBG's Virtual Private Network (VPN) policy and VPN Access Acceptance Form.

(U) BBG Response (October 17, 2014): BBG concurs. **The BBG has recently completed several "Proof of Concepts" to address this weakness. Subject to available funding, the BBG intends to deploy them across all elements of BBG's Washington Network during FY 2015.**

(U) Recommendation 15. OIG recommends that the Enterprise Networks and Storage Division ensure that multiple personnel are trained, and utilize that training, to disable Virtual Private Network tokens after they are reported lost or stolen in accordance with National Institute of Standards and Technology, Special Publication 800-53, Revision 4.

(U) BBG Response (October 17, 2014): BBG concurs. **The BBG will ensure that multiple Customer Systems Support Division (T/SC) staff members are trained and follow consistent procedures when they issue and disable BBG remote access tokens during FY 2015.**

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)

(U) Recommendation 16. OIG recommends that the Director of Global Operations and system owners ensure that user accounts are properly maintained in accordance with Broadcasting Board of Governors' *Identification and Authentication Policy*.

(U) BBG Response (October 17, 2014): BBG concurs. A continuous monitoring program is under development to ensure that authorization and access control is consistently enforced on all domain and local user accounts in accordance with the BBG's user account configuration policy.

(U) Recommendation 17. OIG recommends that the Director of Global Operations, in coordination with the Office of Security, complete the issuance of Personal Identity Verification cards as required by Homeland Security Presidential Directive 12 and Office of Management and Budget guidelines.

(U) BBG Response (October 17, 2014): BBG concurs. The BBG has accelerated issuance of Personal Identity Verification (PIV) cards to its employees and contractors in 2014 and will continue to issue cards at this pace in 2015. In addition, the CIO will continue to assess progress on PIV issuance and expand its usage as part of logical access control within the BBG's network as much as practical within the budget constraints imposed on the Agency.

(U) Recommendation 18. OIG recommends that the Director of Global Operations finalize and implement a role-based security training policy, as required by the National Institute of Standards and Technology Special Publication 800-53, Revision 4.

(U) BBG Response (October 17, 2014): BBG concurs. The CIO will take steps to develop and implement a role-based IT security program, within budgetary limitations, in accordance with guidance from the National Institute of Standards and Technology, during FY 2015.

CONTROLLED UNCLASSIFIED INFORMATION
(UNCONTROLLED when removed from enclosure)



**FRAUD, WASTE, ABUSE,
OR MISMANAGEMENT
OF FEDERAL PROGRAMS
HURTS EVERYONE.**

CONTACT THE
OFFICE OF INSPECTOR GENERAL
HOTLINE
TO REPORT ILLEGAL
OR WASTEFUL ACTIVITIES:

202-647-3320

800-409-9926

oighotline@state.gov

oig.state.gov

Office of Inspector General
U.S. Department of State
P.O. Box 9778
Arlington, VA 22219